COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

JUDI E. THOMAS
CHIEF DEPUTY

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JAMES L. SCHNEIDERMAN

October 25, 2012

TO: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Wendy L. Watanabe Wendy L Watanabe by Schneiderman
Auditor-Controller

SUBJECT: **REVIEW OF LAC+USC MEDICAL CENTER'S COMPLIANCE WITH BOARD INFORMATION TECHNOLOGY AND SECURITY POLICIES**

The Board of Supervisors' Information Technology (IT) and Security Policies (Policies) require all County departments to comply with established County IT security standards. The Policies help ensure proper controls over County IT resources. As required by Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Health Services LAC+USC Medical Center's (LAC+USC or Department) compliance with the Policies, and related County standards and requirements. Our review included testing system access, physical security over IT equipment, computer antivirus and encryption software, equipment disposition, and IT security training.

<u>Results of Review</u>

LAC+USC needs to improve its controls over its system access and IT equipment. For example:

- LAC+USC needs to restrict access to their systems. We reviewed three of over 50 LAC+USC systems containing sensitive information, and noted that LAC+USC had not terminated the system access for eight (44%) of 18 users reviewed who left LAC+USC or changed assignments. One employee's access, which allowed her to change other users' access levels and reset passwords, was used 18 months after she changed assignments. However, because LAC+USC does not keep the system logs, we could not determine how the access was used or what was changed.

In addition, 4,619 (51%) of 8,998 staff who have access to LAC+USC's Pharmacy On The Web (prescription medication) system have never used it, and another 2,390 (27%) have not used their access in over a year.

LAC+USC's attached response indicates they removed the unnecessary access/accounts, and will remove access when employees terminate or change assignments. They also reminded system managers to limit system access, and to document procedures for monitoring administrative users' system log-ons. Although not addressed in their response, LAC+USC should also log and monitor administrative users' system activity.

- LAC+USC needs to ensure that all user log-on identifications (ID) are assigned to specific individuals, and immediately terminate any unassigned IDs. Four LAC+USC systems reviewed had a total of 68 IDs that were not assigned to specific users. These IDs could be used to improperly access confidential information without leaving a record of who accessed the information. Fifteen of the 68 IDs could be used to modify other users' access levels, add/remove patient services from billings, and prescribe medication.

  LAC+USC's response indicates they removed the generic IDs, and reminded system managers to ensure that log-on IDs are assigned to specific individuals.

- LAC+USC's IT equipment inventory records may not be accurate. Specifically, LAC+USC's inventory shows 2,822 computers, but another report shows 6,212 computers have antivirus protection. In addition, we could not locate 16 (73%) of 22 computers we attempted to find. LAC+USC staff later located 15 of the 16 computers.

  LAC+USC's response indicates they created a new equipment inventory database, and inventoried their IT equipment. However, an internal audit performed by the Department identified discrepancies in the new inventory, so they will perform a second inventory. LAC+USC also reminded IT staff to report missing equipment to management immediately, so they can report incidents timely.

- LAC+USC needs to better safeguard IT equipment. We noted LAC+USC does not always properly tag computer equipment, lock/secure desktop computers, close doors to computer storage rooms, or bolt server racks to the wall or floor.

  LAC+USC's response indicates that they will ensure all IT equipment is properly tagged, instructed IT staff to lock computer storage rooms, and will bolt server racks to the floor. They also indicated that it is not economically feasible to purchase locks *for all their computers, and that there is minimal risk for loss/theft. However, we recommend that LAC+USC work with the County's Chief Information Office (CIO) and Internal Services Department (ISD) on lock pricing. At a minimum, LAC+USC should consider securing the most high-risk/vulnerable computers, such as those located in public areas, as required by their Departmental Policy 935.11 Section IV.A.*

- LAC+USC needs to ensure all computers have current, functioning antivirus protection. Ten (53%) of the 19 computers reviewed did not have current antivirus protection, including one with no protection at all.

  LAC+USC's response indicates that they have ensured all computers now have current, functioning antivirus software.

- LAC+USC needs to properly dispose of obsolete computer hard drives. We noted LAC+USC has accumulated hundreds of hard drives, which they have not inventoried, sanitized, or disposed of for many years. In addition, LAC+USC could not document that they sanitized the hard drives from 32 leased photocopy machines that were returned between January 2010 and July 2011, as required by Policy 6.112.

  LAC+USC's response indicates that they have implemented procedures to ensure staff inventory and sanitize obsolete hard drives in IT equipment and leased copy machines before disposing of them. They also indicated that they have instructed IT staff to dispose of the obsolete equipment more frequently.

- LAC+USC needs to protect personal/confidential information on portable devices. LAC+USC management indicated they do not have a process for staff to obtain approval to place confidential information on portable devices, and do not keep records of confidential data on portable devices, as required by Policy 6.110. As a result, LAC+USC would not be able to recreate the data, or notify affected individuals if the data was compromised.

  LAC+USC indicated that they were advised that the County's Chief Information Office is revising Policy 6.110, and that that they will work with the CIO to ensure they comply with the revised Policy, which is expected to be issued in January 2013. They will also encrypt data stored on portable devices to protect the data in case of loss or theft. LAC+USC should also update their Departmental Policy 935.11 Section III.D based on the CIO's revised policy.

Details of these and other findings and recommendations are included in Attachment I. While our review did not disclose any instances of fraud or lost data, the weaknesses noted in this report are serious and, if not corrected, could allow losses to go undetected.

Acknowledgment

We discussed our report with LAC+USC management. LAC+USC's response (Attachment II) indicates general agreement with our findings and recommendations.

We thank LAC+USC management and staff for their cooperation and assistance during our review. Please call me if you have any questions, or your staff may contact Robert Campbell at (213) 253-0101.

WLW:JLS:RGC:MP

Attachments

c: Mitchell H. Katz, M.D., Director, Department of Health Services
William T Fujioka, Chief Executive Officer
Robert Pittman, Chief Information Security Officer, Chief Information Office
Public Information Office
Audit Committee

ATTACHMENT I

DEPARTMENT OF HEALTH SERVICES
LAC+USC MEDICAL CENTER
INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW

Background

The Board of Supervisors' Information Technology (IT) and Security Policies (Policies) require all County departments to comply with minimum IT security standards. The Policies help ensure proper controls over the privacy and confidentiality, integrity, availability, and appropriate use of County IT resources and data. As required by Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of Department of Health Services (DHS) LAC+USC Medical Center's (LAC+USC or Department) compliance with the Policies and related County standards and requirements. Our review included testing physical security, antivirus and encryption software, equipment disposition, access to sensitive data, and user information security awareness training.

Access Controls

Unnecessary System Access

Policy 3.040 requires departments to restrict system access to staff who need it for their work. County Fiscal Manual (CFM) Section 8.6.4 also requires departments to periodically review user access to ensure it is authorized and appropriate. These controls help ensure accountability, and the integrity of IT data.

We reviewed user access to three of over 50 critical LAC+USC systems; the Pharmacy On The Web (prescription medication), Synapse (patient x-ray), and computer antivirus software management systems, and noted users who had unneeded access. Specifically:

- Eight (44%) of the 18 users reviewed no longer work at LAC+USC, or changed assignments and no longer needed system access. One employee's access, which could be used to change other users' access levels and reset passwords, was used 18 months after she changed assignments. However, because LAC+USC does not keep comprehensive system activity logs, we could not determine how the access was used or what was changed.

- 4,619 (51%) of the 8,998 active user IDs in the prescription medication system had never been used, and another 2,390 (27%) had not been used in over a year.

- 779 users of the prescription medication and patient x-ray systems had two or more log-on identifications (IDs). No user should have more than one log-on ID for any system.

To reduce the risk of unauthorized access and inappropriate activity, LAC+USC management should only grant system access when needed; immediately remove unnecessary access; ensure access is canceled when employees leave or change assignments; and review access regularly to ensure assignments and changes are appropriate. LAC+USC management should also log and monitor users with higher-level access to help detect any inappropriate activity, as required by CFM Section 8.6.4.

Recommendations

LAC+USC management:

1. **Ensure system access is granted only when needed.**

2. **Immediately remove unnecessary system access; cancel access when employees terminate or change assignments; and review system access regularly.**

3. **Log and monitor users with higher-level access.**

Unassigned User Log-on Identifications

Policy 6.101 requires that systems have appropriate user authentication, such as log-on IDs and passwords, to identify and authenticate each user.

We noted LAC+USC's prescription medication, patient x-ray, and computer antivirus software management systems, as well as the Department's network log-on, all have some generic IDs that are not assigned to individual employees, and can be used to access sensitive/confidential information with no record of who used them. Specifically:

- The prescription medication and patient x-ray systems each have approximately 30 generic IDs that are sometimes shared among employees. Thirteen (38%) of 34 generic IDs in the system can be used to prescribe medication (except for narcotics), and two generic IDs in each system can modify user access levels and alter patients' bills.

- The Department's computer antivirus software management system and network log-on each have at least one generic ID that is shared among employees.

Generic user IDs increase the risk of fraud and unauthorized activity. To establish accountability over user activity, LAC+USC should immediately delete any generic/unassigned user IDs, and ensure all user IDs are assigned to specific authorized individuals. LAC+USC should also review all transactions using generic IDs to verify they are appropriate, and identify the staff who created and used these IDs to determine if they were authorized to have that level of access.

Recommendations

LAC+USC management

4. **Ensure all system log-on identifications are assigned to specific individuals.**

5. **Immediately delete generic/unassigned user IDs.**

6. **Review all transactions from generic IDs to verify they are appropriate, and identify staff who created and used the IDs to determine if they were authorized to have that level of access.**

Physical Security

IT Inventory

CFM Section 6.8.2 requires departments to maintain an up-to-date IT equipment inventory to help safeguard the equipment from loss, damage, or theft.

LAC+USC does not have a current or accurate inventory of IT equipment, and it appears that a significant number of computers may be unaccounted for. Specifically, LAC+USC's inventory shows 2,822 computers, but another report shows 6,212 computers have antivirus software protection. We selected 22 computers from inventory, and could not locate 16 (73%) of them. LAC+USC staff later found fifteen of the 16 computers.

LAC+USC management acknowledged that they did not inventory equipment before or after moving to the new hospital in 2008, which could indicate that the unaccounted for computers may have been lost in the move.

LAC+USC management should inventory their IT equipment immediately, and annually thereafter, as required by CFM Section 6.8.2. Department management should also investigate and report any missing computers to the Auditor-Controller's Office of County Investigations, and Chief Information Office as required by Policy 6.109.

Recommendations

LAC+USC management:

7. **Inventory IT equipment immediately, and annually thereafter.**

8. **Investigate and report any missing computers.**

Controls over Confidential Information

Policy 6.110 requires departments to ensure staff obtain written management approval to place confidential information on portable devices. The Policy also requires departments to ensure that they can recreate confidential information, and notify affected individuals if it is lost or stolen.

LAC+USC management indicated that they do not have a process in place for staff to obtain approval to place confidential information on portable devices. Management also told us that they do not have records of the confidential information on the portable devices. As a result, LAC+USC could not recreate the information, or notify the affected individuals, if the information were compromised.

We also noted that LAC+USC is not using the computer port control (which prevents unauthorized portable devices from accessing County data), and email encryption software licenses the facility has. Specifically, LAC+USC has not used:

- 3,350 computer port control software licenses they purchased in April 2009, at a total cost of $42,377. They also pay over $7,000 per year to renew these licenses.
- 500 email encryption licenses obtained from the Chief Information Office, at no cost, to help reduce the risks associated with emailing confidential records.

LAC+USC management told us that they have not used the software because they encountered software conflicts and other issues during the installation. However, they have not developed a plan to resolve the issues, and continue to pay the annual renewal fees for the unused software.

To ensure personal/confidential information is protected, LAC+USC management needs to implement the following recommendations.

Recommendations

LAC+USC management:

9. Establish a process for staff to obtain written management approval to place personal/confidential information on portable devices.

10. Maintain a record of the confidential information on portable devices, and ensure that it can be recreated so that affected individuals can be notified if the information is compromised.

11. Develop a plan to resolve email encryption/computer control software issues, and install the software where possible/practical.

12. **Discontinue paying maintenance and renewal fees for unused software.**

Equipment Security

We noted the following other IT equipment control weaknesses where the Department is not complying with the Policies and CFM requirements:

- LAC+USC's IT equipment inventory list does not always have accurate or required information, such as serial or asset tag numbers.
- LAC+USC does not always tag County IT equipment; lock/secure desktop computers; close doors to computer storage rooms; or bolt server racks to the wall or floor to prevent damage in an earthquake.
- LAC+USC staff do not always wear their identification badges to help prevent unauthorized access, and safeguard assets from accidental loss, damage, or theft.

LAC+USC management should strengthen physical security and controls over equipment by implementing the following recommendations.

Recommendations

LAC+USC management:

13. **Ensure the IT equipment inventory list contains accurate, required information.**
14. **Ensure County IT equipment is properly tagged.**
15. **Lock/secure desktop computers and computer storage rooms.**
16. **Bolt unsecured server racks to the wall or floor.**
17. **Ensure staff wear ID badges.**

Antivirus Software

Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus software protection for all County computers. Ten (53%) of the 19 computers reviewed did not have current antivirus software protection, including one with no protection, and another where the protection could be disabled by the user. For an additional six (32%) computers, certain security features were not operating properly.

LAC+USC management should ensure all computers have current antivirus protection that users can not disable, and that IT staff resolve the software issues that are preventing security features from operating properly.

Recommendations

LAC+USC management:

18. Ensure all computers have current antivirus protection that users cannot disable.

19. Ensure IT staff promptly resolve the software issues that are preventing security features from operating properly.

Secure Disposal of Computing Devices

CFM Section 5.2.6 requires departments to monitor inventory records and dispose of obsolete items. Policy 6.112 and the Hard Drive Cleaning Standard require departments to erase all data/software from IT equipment (sanitize) before disposal, and to document that each device was sanitized.

LAC+USC has accumulated hundreds of obsolete computer hard drives containing County data/software, which they have not sanitized or disposed of in a number of years. They also have not inventoried the hard drives, which increases the risk for loss of personal/confidential information. LAC+USC also could not document whether they sanitized 32 leased photocopy machine hard drives that were returned to the lessors between January 1, 2010 and July 14, 2011.

To prevent unauthorized use or disclosure of County information, LAC+USC management needs to implement the following recommendations.

Recommendations

LAC+USC management:

20. Immediately inventory, sanitize, and dispose of the obsolete hard drives.

21. Monitor and dispose of obsolete equipment timely.

22. Sanitize IT equipment and leased copy machines before disposing of them, and retain documentation that they are sanitized.

IT Security Awareness Training

Policy 6.111 requires departments to provide IT Security Awareness Training to all users (County and non-County) of County IT resources to ensure they are aware of the Policies, and their responsibilities for information security. Departments should document that employees completed the training.

LAC+USC does not provide the required training. Management told us they train new staff at orientation, and provide all staff with IT security tips using email/screen messages. However, the training does not always cover, or help staff understand, IT security issues, such as the appropriate use of County IT resources, and the required process for reporting security incidents. In addition, LAC+USC could not document who received the security tips, and some of the tips were missing key content, such as training on malicious software, and the disposal of electronic data as noted in the Department's security training policy

LAC+USC management should ensure all IT users receive adequate IT security training, and that the training is properly documented.

Recommendation

23. LAC+USC management ensure all IT resource users receive adequate IT Security Awareness Training, and that the training is properly documented.

IT Risk Assessment

Policy 6.107 requires departments to identify critical IT services, and assess their information security risks as part of the Auditor-Controller's Internal Control Certification Program (ICCP). Departments must certify that proper controls are in place, or that action is being taken to correct any weaknesses or vulnerabilities.

Many of the weaknesses/vulnerabilities noted in our review should have been detected when LAC+USC completed their ICCP. However, LAC+USC's most recent certification indicated that the appropriate controls were in place.

To help LAC+USC managers evaluate and improve internal controls over IT and security, management should perform and document information security risk assessments by properly completing the ICCP.

Recommendation

24. LAC+USC management perform and document information security risk assessments by properly completing the Internal Control Certification Program.

ATTACHMENT II

Health Services
LOS ANGELES COUNTY

313 N. Figueroa Street, Suite 912
Los Angeles, CA 90012

Tel: (213) 240-8101
Fax: (213) 481-0503

www.dhs.lacounty.gov

To ensure access to high-quality, patient-centered, cost-effective health care to Los Angeles County residents through direct services at DHS facilities and through collaboration with community and university partners.

www.dhs.lacounty.gov

October 2, 2012

TO: Wendy L. Watanabe
Auditor-Controller

FROM: Mitchell H. Katz, M.D.
Director

SUBJECT: **RESPONSE TO AUDITOR-CONTROLLER'S REVIEW OF INFORMATION TECHNOLOGY AND SECURITY POLICIES COMPLIANCE AT LAC+USC MEDICAL CENTER (LAC+USC MC)**

Attached is the Department of Health Services' response to the recommendations made in the Auditor-Controller's report of its review of Information Technology and Security Policies Compliance at LAC+USC MC. We generally agree with and have taken or initiated corrective actions to address the recommendations in the report.

If you have any questions or require additional information, please let me know or you may contact Tobi L. Moree at (213) 240-7901 or Elizabeth Guzman at (213) 240-7759.

MHK:tlm:eg

Attachment

c: Kevin Lynch
Oscar Autelli
Pete Delgado
Gregory Polk

COUNTY OF LOS ANGELES – DEPARTMENT OF HEALTH SERVICES (DHS)
RESPONSE TO AUDITOR-CONTROLLER - COMPLIANCE WITH BOARD
INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW
LOS ANGELES COUNTY + USC MEDICAL CENTER (LAC+USC MC)

AUDITOR-CONTROLLER RECOMMENDATION #1

LAC+USC MC management ensure system access is granted only when needed.

DHS response:

We agree. On September 19, 2012, LAC+USC MC Departmental Information Security Officer (DISO) sent an e-mail containing DHS Information Access Management Policy No. 935.04, to LAC+USC MC System Managers/Owners. The policy indicates that System Managers/Owners should authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the workforce. The e-mail also instructed the System Managers/Owners that written procedures are required for all DHS IT policies. The LAC+USC MC DISO will continue to conduct internal risk assessment audits to ensure that all DHS IT policies along with the system access granting policy are strictly enforced.

AUDITOR-CONTROLLER RECOMMENDATION #2

LAC+USC MC management immediately remove unnecessary system access, cancel access when employees terminate or change assignments, and review system access periodically.

DHS response:

We agree. In February 2011, an extensive review of critical applications was conducted by the LAC+USC MC DISO to ensure unnecessary user accounts are not utilized and are eliminated. As a result of this review, unnecessary system access (duplicate and generic user accounts) was eliminated from the audited applications, Pharmacy on the Web, SEP11, and Synapse. The LAC+USC MC DISO will continue to conduct reviews of critical applications semi-annually to verify that the remaining critical applications do not have any unnecessary user accounts. If deficiencies are found, the LAC+USC MC DISO will notify System Managers/Owners to eliminate unnecessary system access.

Effective March 26, 2010, LAC+USC MC automated its “Exit Interview Notification”. Upon receipt of a list of terminated employees from DHS Human Resources (HR), a Help Desk ticket is automatically generated and assigned to LAC+USC MC System Managers/Owners to disable the terminated user's system access. Additionally, effective October 31, 2012, the "Facility Sign Out" process will be enhanced to automatically route notifications to the Help Desk ticketing system directing all critical application System Managers/Owners to cancel terminated employee's access. LAC+USC MC IT Operations is currently working with DHS IT Applications and Development to further ensure that DHS HR provides a change assignment list (change role) to Information Technology (IT), and/or generates an automated "Assignment Change Notification" in order to remove unnecessary system access when employees change assignments.

System Managers/Owners are required to check and disable the inactive user accounts and review system access periodically. The LAC+USC MC DISO will audit the System Managers/Owners documentation to ensure that they are reviewing the system access logs periodically. Also critical applications are set to a three-month password change policy, whereby if a user does not change her/his password by the assigned date, the account will be disabled.

AUDITOR-CONTROLLER RECOMMENDATION #3

LAC+USC MC management logs and monitors users with higher-level access.

DHS response:

We agree. By September 13, 2012, all unnecessary administrative user accounts were removed from the audited applications (Pharmacy on the Web, Symantec Endpoint Protection 11.0 (SEP11), and Synapse), and administrative access has been restricted to limited staff only. On September 19, 2012, the LAC+USC MC DISO sent an e-mail to the System Managers/Owners instructing them that written procedures are required for all DHS IT policies, and specifically mentioned DHS System Audit Controls Policy No. 935.14. DHS Policy No. 935.14 states "system log-in monitoring: user and process access to system must be recorded and monitored for successful and failed attempts".

AUDITOR-CONTROLLER RECOMMENDATION #4

LAC+USC MC management ensure all system log-on identifications (IDs) are assigned to specific individuals.

DHS response:

We agree. On September 19, 2012, the LAC+USC MC DISO sent an e-mail to the System Managers/Owners instructing them that written procedures are required for all DHS IT policies, and specifically mentioned DHS No. 935.14.

DHS Policy No. 935.14 states DHS systems must assign a unique name and/or number to each user for identifying and tracking user identity, to ensure that system log-on IDs are assigned to specific individuals.

AUDITOR-CONTROLLER RECOMMENDATION #5

LAC+USC MC management immediately delete generic/unassigned user IDs.

DHS response:

We agree. Effective September 14, 2012, generic/unassigned user IDs have been disabled from Pharmacy on the Web and Synapse Radiology systems. LAC+USC MC Information Security Office reviews selected applications user access logs semi-annually to ensure no generic/unassigned accounts are created. Although System Managers/Owners are required to check the inactive user accounts and disable them, because of the large number of application users in our facility, it is almost impossible for System Managers/Owners to review system access logs regularly. To mitigate this issue, critical applications are set to a three-month password change policy, whereby if a user does not change her/his password by the assigned date, the account will be disabled. Generic/unassigned user IDS will be disabled from remaining applications by June 30, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #6

LAC+USC MC management review all transactions from unassigned IDs to verify they are appropriate, and identify staff who created and used the IDs to determine if they were authorized to have that level of access.

DHS response:

We partially agree. Although most applications do not have the capability of identifying staff who created unassigned user IDs, only application administrators are authorized to create unassigned IDs. By December 30, 2012, LAC+USC MC will work with application System Managers/Owners to conduct a sample audit of transactions from unassigned IDs to verify whether they are appropriate.

AUDITOR-CONTROLLER RECOMMENDATION #7

LAC+USC MC management inventory Information Technology (IT) equipment immediately, and annually thereafter.

DHS response:

We agree. A new equipment inventory database (INVPC) was created in May 2011, and IT Operations Staff inventoried IT equipment in June 2011; however an internal audit found discrepancies. A new inventory of IT equipment will be completed by March 31, 2013, and annually thereafter.

AUDITOR-CONTROLLER RECOMMENDATION #8

LAC+USC MC management investigate and report any missing computers.

DHS response:

We agree. On January 12, 2012, IT staff were re-instructed to immediately report any missing equipment to management and the LAC+USC MC DISO so that an incident report can be prepared in a timely manner. LAC+USC MC follows DHS Security Incident Report and Response Policy No. 935.06, which states "DHS Workforce Members are required to immediately report theft or loss of hardware to the facilities IT Department, the facility IT service desk, facility Information Security Coordinator, facility Privacy Coordinator, and DHS Security and Compliance Division, who will investigate and as needed refer to others". The procedures include the completion of the DHS Incident Report form. IT staff investigated and found 10 (91%) of the 11 computers that were missing at the time of audit. Photographic documentation of recently found computers will be provided to the auditor By December 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #9

LAC+USC MC management establish a process for staff to obtain written management approval to place personal/confidential information on portable devices.

DHS response:

We disagree. The County Information Security Officer (CISO) is currently revising Board of Supervisor Protection of Information on Portable Computing Devices Policy No. 6.110, which will no longer include the instruction to obtain written management approval to place personal/confidential information on portable devices; the target date for the revised policy is January 2013. LAC+USC MC will work with the CISO to ensure compliance with the revised policy. LAC+USC MC is also in the process of implementing Safend, a portable device encryption solution, which will encrypt data stored on USB thumb drives as well as other portable devices, to ensure that the data is protected in case of loss or theft. The target completion date for this project is December 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #10

LAC+USC MC management maintain a record of the confidential information on portable devices, and ensure that it can be recreated so that affected individuals can be notified if the information is compromised.

DHS response:

We disagree. The CISO is currently revising Board of Supervisors Policy No. 6110, with an estimated completion date of January 2013. LAC+USC MC will work with the CISO to ensure compliance with the revised policy. LAC+USC MC is also in the process of implementing Safend, a portable device encryption solution, which will encrypt data stored on USB thumb drives as well as other portable devices, to ensure that the data is protected in case of loss or theft. The target completion date for this project is December 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #11

LAC+USC MC management develop a plan to resolve e-mail encryption/computer control software issues, and install the software where possible/practical.

DHS response:

We agree. LAC+USC MC initiated the DHS e-mail encryption solution in February 2012, and IT personnel continue to add workforce members' names to the e-mail encryption bucket. The computer port control project (Safend) is in progress and the target completion date is December 31, 2012. The success of this project is contingent upon receiving the requested additional computer agent licenses from DHS.

AUDITOR-CONTROLLER RECOMMENDATION #12

LAC+USC MC management discontinue paying maintenance and renewal fees for unused software.

DHS response:

We agree. Beginning February 2012, LAC+USC MC started installing and implementing the DHS e-mail encryption software solution. Also, the computer port control project (Safend) is in progress, with a target completion date of December 31, 2012. LAC+USC MC will use software licenses and have requested additional computer agent licenses from DHS IT. In the future, LAC+USC MC management will not pay maintenance and renewal fees for unused software.

AUDITOR-CONTROLLER RECOMMENDATION #13

LAC+USC MC management ensure the IT equipment inventory list contains accurate, required information.

DHS response:

We agree. A new equipment inventory database (INVPC) was created in May 2011. IT Operations re-inventoried all desktops and laptops in June 2011. IT Operations Staff were instructed and mandated in weekly and monthly staff meetings to maintain the accuracy of the database. DHS Policy No. 935.13 was implemented and procedures were introduced in order to ensure IT Operations - PC Support Staff actively check, amend and add devices to the inventory database. The database will be updated when new equipment is received, obsolete equipment is replaced or existing equipment is relocated. This process is validated and cross-checked by the LAC+USC MC Procurement Coordinator, who audits the INVPC database weekly by double-checking the work orders and tickets in FootPrints, the ticketing system, against the INVPC. The LAC+USC MC DISO conducts random internal audits to verify the accuracy of the equipment inventory. The LAC+USC MC IT Operations Supervisor is responsible to rectify any discrepancies.

AUDITOR-CONTROLLER RECOMMENDATION #14

LAC+USC MC management ensure County IT equipment is properly tagged.

DHS response:

We agree. Beginning in May 2011, LAC+USC MC Operations staff has been re-assessing all IT computing equipment to ensure that they are properly tagged;

the target completion date is June 2013. Existing IT equipment that is out of warranty will be replaced and the replacement equipment will be properly tagged.

AUDITOR-CONTROLLER RECOMMENDATION #15

LAC+USC MC management lock/secure desktop computers and storage rooms.

DHS response:

We partially agree. LAC+USC MC has more than 6,500 desktop computers, and it is economically unfeasible to purchase and install lockdown devices for all of them; purchase cost of approximately $650,000, not including labor. In February 2012, IT Operations staff were instructed to keep computer storage rooms locked at all times and to ensure that storage rooms are accessible only by certain authorized personnel. Most offices are accessible only to staff who have received keys. In other publicly accessible areas, workstations are in operation 24 hours per day and seven days per week (24/7) with staff present at all times. Additionally, safety officers are also deployed on a 24/7 basis throughout the hospital.

AUDITOR-CONTROLLER RECOMMENDATION #16

LAC+USC MC management bolt unsecured server racks to the wall or floor.

DHS response:

We agree. By December 31, 2012, IT Operations will work with the Office of Facilities Management to secure all unsecured Outpatient Department (OPD) data center server racks by bolting them to the floor.

AUDITOR-CONTROLLER RECOMMENDATION #17

LAC+USC MC management ensure staff wear ID badges.

DHS response:

We agree. DHS Policy No. 940, Identification Badges, effective May 19, 2004, indicates it is the responsibility of personnel to wear ID badges at all times while on County premises. As part of the annual performance evaluation process, each DHS employee signs an acknowledgment form that they have read, reviewed and will comply with a list of policies, including DHS Policy No. 940. On

September 24 and 26, 2012, e-mails were sent to LAC+USC IT Staff instructing them that employees must wear the County issued badge at all times while on County premises during working hours as required by DHS Policy No. 940.

AUDITOR-CONTROLLER RECOMMENDATION #18

LAC+USC MC management ensure all computers have current antivirus protection that users cannot disable.

DHS response:

We agree. Only older versions of Symantec software permitted users to disable malware protection software. All older Symantec versions have been updated to a newer version of Symantec Endpoint Protection 11.7 (SEP11), beginning with the first deployment in January 2009 and was completed on October 11, 2011. Permissions to disable malware protection or change software configuration have been disabled with this version. Currently, a group policy is pushed through Active Directory to install the SEP11 agent to all workstations that are joined to the domain.

AUDITOR-CONTROLLER RECOMMENDATION #19

LAC+USC MC management ensure IT staff promptly resolve the software issues that are preventing security features from operating properly.

DHS response:

We agree. In November 2011, one designated LAC+USC MC IT staff was assigned to actively monitor and resolve malware defense software issues that were preventing security features from operating properly. Most instances were mitigated by upgrading to SEP11.

AUDITOR-CONTROLLER RECOMMENDATION #20

LAC+USC MC management immediately inventory, sanitize, and dispose of the obsolete hard drives.

DHS response:

We agree. LAC+USC MC Information Systems Operation Support Procedure, Device and Media Control Procedure, effective April 5, 2011, related to DHS

Policy No. 935.13 was reviewed and implemented in July 2011 to ensure that IT Operations (PC Support) staff inventory and sanitize obsolete hard drives before disposing of them.

AUDITOR-CONTROLLER RECOMMENDATION #21

LAC+USC MC management monitor and dispose of obsolete equipment timely.

DHS response:

We agree. On August 22, 2012, LAC+USC MC IT Operations was instructed by the LAC+USC DISO to dispose of the obsolete equipment in a timely manner. LAC+USC MC Information Systems Operation Support Procedure, Device and Media Control Procedure, effective April 5, 2011, related to DHS Policy No. 935.13 was reviewed and implemented on July 2011 to ensure that PC Support staff inventory and sanitizes obsolete equipment timely. In June 2011 The IT Operations supervisor began monitoring the salvaged equipment process on a weekly basis.

AUDITOR-CONTROLLER RECOMMENDATION #22

LAC+USC MC management sanitize IT equipment and leased copy machines before disposing of them, and retain documentation that they are sanitized.

DHS response:

We agree. LAC+USC MC Information Systems Operation Support Procedure, Device and Media Control Procedure, effective April 5, 2011, related to DHS Policy No. 935.13 was reviewed and implemented in July 2011 to ensure that IT Operations (PC Support) staff inventory and sanitize obsolete hard drives before disposing of them. LAC+USC MC IT Operations will sanitize IT equipment and leased copy machines (multi-function printers) before disposal and maintain documentation for IT equipment. LAC+USC MC SCO Property Management Unit will retain documentation that leased copy machines were sanitized prior to disposal or return to vendor. In November 2011, DHS Supply Chain Operations (SCO) worked with DHS IT and each DHS hospital's IT to return 141 leased copy machines to the vendor. DHS IT worked with each hospital's IT to ensure the Central Processing Unit (CPU) was pulled out from each machine, replaced, and later all CPUs were sanitized.

AUDITOR-CONTROLLER RECOMMENDATION #23

LAC+USC MC management ensure all IT resource users receive adequate IT Security Awareness Training, and that the training is properly documented.

DHS response:

We agree. DHS HR is currently in the process of conducting comprehensive compliance training for all LAC+USC MC workforce members. The training covers privacy and security areas, which will be properly documented in the County Learning Management System (LMS). Instructor-led training is also available for workforce members who do not have access to a computer. The target date of completion of this training is December 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #24

LAC+USC MC management perform and document information security risk assessments by properly completing the Internal Control Certification Program (ICCP).

DHS response:

We agree. LAC+USC MC will perform and document information security risk assessments by properly completing the ICCP's for one critical application each year, which will be prepared and submitted annually beginning May 15, 2013.